2-16-00 A/PRov

In the United States Patent and Trademark Office

Box Provisional Patent Application
Assistant Commissioner for Patents
Washington, District of Columbia 20231

Mailed February 15, 2000

Sir:

Please file the enclosed Provisional Patent Application (PPA) papers listed below under 37 C.F.R. § 1.53(b)(2).

The undersigned understands:

A. This PPA is not a substitute for a Regular Patent Application (RPA), cannot be converted to an RPA, cannot get into interference with an RPA of another person, cannot be amended, will not be published, cannot claim any foreign priority, and will not mature into a patent;
B. If an RPA referring to this PPA is not filed within one year of the filing date of this PPA, this PPA will be worthless and will be destroyed;
C. Any desired foreign Convention applications (including PCT applications) based upon this PPA must be filed within one year of the filing date of this PPA;
D. This PPA must contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention. 35 U.S.C. § 112, ¶ 1. Otherwise this PPA will be worthless.
E. Any RPA will be entitled to claim the benefit of this PPA only if such RPA names at least one inventor of this PPA and this PPA discloses such inventor's invention, as claimed in at least one claim of the RPA, in the matter provided in Item D above.

Tentative Applicant Name:
Brian L. Whitworth

Title:
Fraud Resistant Credit Card Using Encryption

(x) Specification, sheets: 18
(x) Drawing(s), sheets : 7
(x) Provisional Claims, sheets: 2
(x) Small Entity Declaration(s), number: 1
(x) Check for $ 75 for (x) small entity ( ) large entity filing fee

Very respectfully,

Brian L. Whitworth
3003 Sequit Dr.
Malibu, CA 90265

Express Mail Label # EK388250281US
Date of Deposit: February 15, 2000

In the United States Patent and Trademark Office

First/Sole Applicant: Brian L. Whitworth

Title: "Fraud Resistant Credit Card Using Encryption"

Small Entity Declaration—Independent Inventor(s)

As a below-named inventor, I hereby declare that I qualify as an independent inventor as defined in 37 CFR 1.9(c) for purposes of paying reduced fees under Section 41(a) and (b) of Title 35 United States Code, to the Patent and Trademark Office with regard to my above-identified invention described in the specification filed herewith. I have not assigned, granted, conveyed, or licensed—and am under no obligation under any contract or law to assign, grant, convey, or license—any rights in the invention to either (a) any person who could not be classified as an independent inventor under 37 CFR 1.9(c) if that person had made the invention, or (b) any concern which would not qualify as either (i) a small business concern under 37 CFR 1.9(d) or (ii) a nonprofit organization under 37 CFR 1.9(e).

Each person, concern, or organization to which I have assigned, granted, conveyed, or licensed—or am under an obligation under contract or law to assign, grant, convey, or license—any rights in the invention is listed below:

(x) There is no such person, concern, or organization.
( ) Any applicable person, concern, or organization is listed below: *

Full Name: Brian L. Whitworth
Address: 3003 Sequit Dr., Malibu, CA 90265

I acknowledge a duty to file, in the above application for patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate (37 CFR 1.28(b)).

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

Signature of Sole/First Inventor

Brian L. Whitworth
Print Name of Sole/First Inventor Print Name

February 15, 2000
Date of Signature

FRAUD RESISTANT CREDIT CARD USING ENCRYPTION

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to credit cards, debit cards and ATM cards which have improved resistance to fraud and theft using encryption and time codes within the cards themselves. A second embodiment is included for similar cards which are designed to provide identification or security access. A third embodiment is included for using similar procedures to enhance security for internet or local area network password access.

Description of the Related Art

Smart Cards

Currently, smart cards perform a variety of tasks. These cards are able to store information which may change over time, such as the amount of value left on the card for a prepaid phone card or a person's security clearance.

Smart cards use a variety of methods of confirming identification. At this time, however, smart cards do not directly display data in a form which can be read by both humans and machines. The cards must be placed in some form of device or reader in order to extract data which changes over time, such as the remaining balance on the card.

Some smart cards, particularly those used for identification at specified sites, use a physical characteristic of the cardholder to confirm identification (e.g., fingerprints Abtahi, et al, US5509083). In some cases, a data regarding the characteristic is recorded on the card itself. In other cases, that data is stored remotely.

Credit Cards

Credit card theft and fraud cost billions of dollar each year in the United States alone. Numerous attempts have been made to create credit cards which lower the incidence of theft and fraud. Most of this art consists of confirming the identity of the cardholder.

Bar Codes

Bar codes have been successful for a number of uses. They are easily readable by machines from many angles and in a broad range of temperature, humidity, and electric and magnetic field conditions. Bar codes also typically include numbers readable by humans which match the bar codes which are readable by machines. This leads to a convenient backup system in case a bar code reader is not working properly or the bar code is partially smeared or otherwise obscured. These factors have led to widespread use of bar codes and bar code equipment in retail stores.

Common uses of bar codes include pricing, inventory, and identification of merchandise. Special bar codes are used for books and magazines, under the ISBN standard. Other bar codes have been adapted for mailing and addressing. In some cases, bar codes have been used as a method of identification, such as the Ralph's Club cards issued by Ralph's Groceries. In those cases where bar codes have been used for identification, they serve as an alternative to keying in a sequence of numbers or reading a magnetic stripe. Bar codes currently are printed on paper or similar media and when used on identification do not change from one use of the card to the next use of the same card.

Problems with Current Methods of Confirming Identity of Cardholders

Current methods of confirming the identity of a cardholder suffer from at least one of the following problems.

1) The method of confirming identity is dependent on the clerk, cashier, telemarketer, waiter, or other person accepting the card. In-person confirmations, such as showing a photo ID are subject to the honesty and skill level of the person accepting the card. In many instances, the person accepting the card is the same person who will attempt to defraud the credit card company. Thus, a cashier with a stolen credit card number is often able to circumvent the normal verification process. In other instances, busy or poorly trained personnel will simply do a poor job of following normal

verification procedures. Criminals are well aware of this and will often choose particular stores or times when verification is likely to be lax to attempt credit card fraud.

2) The method of confirming identity usually works in person, but is difficult or impossible over the phone or the Internet. A common example of this problem is the inability to check a photo ID or fingerprint over the phone or the Internet without special additional equipment. This can lead to unauthorized charges by persons who would never be mistaken for the real cardholder, such as a 10 year-old girl who has "borrowed" her mother's card without her knowledge and ordered merchandise over the Internet.

3) The method of confirming identity usually works over the Internet, but not over the phone or in person.

4) The method of confirming identification is subject to being circumvented by someone looking over the cardholder's shoulder, or being overheard. A common example is seeing someone's PIN number as they key it in at the grocery checkout lane. If a criminal is also able to get a discarded receipt or see the credit card number, they may be well on their way to fraudulent charges on a card they have never touched.

5) Certain methods of confirming identification using physical characteristics of the cardholder are subject to creative copying or circumvention. For example, some fingerprint verification systems have been defeated by use of a copy of a fingerprint from the cardholder. A typical wallet will not only contain credit cards and identification, but also several retrievable fingerprints on the wallet and its contents. Using evaporation of super glue, a technique pioneered by law enforcement, criminals can extract fingerprint information from paper, leather, plastic and many other surfaces. Many of the places from which a credit or identification card might be stolen contain dozens of retrievable fingerprints. A house, office or car will usually be virtually covered in useable fingerprints.

6) The method of confirming identity may require devices which are expensive or are not widely used.

7) The card number and/or identifying information can be intercepted during the verification process by persons who are not physically present. A large amount of the prior art attempts to deal with this problem by making the transmission of the data secure (e.g., Rowney, et.al., US5987140), rather than using a method of verification which makes intercepted data from one charge useless for a later attempted charge.

8) Repositories of credit card numbers retained for the convenience of cardholders (e.g., internet account numbers at ____ who recently had a whole database of credit card numbers stolen), can sometimes be broken into and huge numbers of customers can be defrauded at once.

Problems with the Cards Themselves

Typical current credit cards have at least one of the following problems:

1) The credit card's magnetic strip can be copied with a simple device. Making copies in this manner is as easy as using a Xerox machine to copy a page of text. Thus, a second card could be used in parallel to the first. If the original card is still in the possession of the cardholder, they may think nothing is wrong until the credit card company calls or they receive an unusually high bill. This is also a weakness of encoding physical information on the card's magnetic strip. The data on the strip can be read and imitated, such as with a fingerprint.

2) The credit card information is displayed at all times, regardless of whether it is in the possession of the cardholder: anyone who can look over your shoulder, see an open wallet, or snoop in an unattended purse can read and copy the necessary cardholder name, account number, and expiration date.

3) If the necessary information is copied and someone attempts fraudulent charges, the original card must be cancelled and a new one issued before the cardholder can resume normal use of their account. This can be a major cause of inconvenience during the time it takes to reissue a card.

4) The credit card itself provides exactly the same information each time it is presented for payment. Thus, anyone able to get the necessary information once is likely to be able to make several charges before anyone notices, even if the thief does not have the card itself.

5) Credit cards accommodate one account per card. Thus, many people carry many different cards which have different purposes or are issued by different institutions.

Typical current smart cards have at least one of the following problems:

1) Smart cards do not directly display data in a form which can be read by both humans and machines. The cards must be placed in some form of device or reader in order to extract data which changes over time, such as the remaining balance on the card. This prevents smart cards from being easily used by humans for phone orders. Special readers are necessary for usage with Internet orders.

2) Smart card readers vary considerably. Currently, the data on smart cards which changes from one use to another is not displayed in bar code fashion.

Social Security, Driver's Licenses, Access Cards and Other Identification

A second embodiment is included for identification cards. The average person has several forms of identification which are not directly used for financial transactions. Most American adults have a social security card and a driver's license. Many also have a passport or identification for their workplace or educational institution. For all of these forms of identification, it is possible for other persons to cause considerable damage by making forged copies or unauthorized duplicates of the original. For example, a fake social security card can be used to get a real driver's license from the state with the thief's picture and handwriting. After obtaining the driver's license, the thief can obtain credit cards or loans using the real person's credit. He may also drive drunk, get married, or conduct other activities which can be very hard for the real person to find and correct in the public record.

Any of these pieces of identification can be replaced by a card similar to the credit, debit or ATM cards described in the primary embodiment. Such identification and methods of verification would render fake documents created without copying real documents virtually useless. Such identification would also be much harder to copy from a real document, since the real document must be in the possession of the forger and much of the critical information is difficult or impossible to access without damaging the original.

Internet or Local Area Network Access Control

A third embodiment is included for internet or local area network password access. This embodiment is provided for confirming the identity of users who wish to access sites or systems via the internet or a local area network. For many systems, especially those involving financial transactions, intercepting a password may allow an unauthorized person to perform transactions as if they were the real user. This ability to intercept information and perform financial transactions on someone else's account has many characteristics in common with credit card fraud. Time sensitive encryption code access provides increased security for internet or LAN access in a manner similar to that described in the primary embodiment for credit cards, debit cards and ATM cards.

Accordingly, it is an object of the present invention to provide a method for creating credit cards, debit cards, and ATM cards which are resistant to fraud or theft by any means where credit card information from prior transactions are obtained.

It is another object of the present invention to provide a method for improved security of access to the card.

It is another object of the present invention to provide improved security and fraud protection for identification such as driver's licenses, Social Security cards, passports, and building access cards.

It is another object of the present invention to provide a method of accessing internet sites using a program which provides information in a manner which reduces

chances of fraud or theft by any means where login, password, or identification information from prior transactions are obtained.

SUMMARY OF THE INVENTION

In accordance with an exemplary preferred embodiment of the present invention, a fraud-resistant credit card using encryption and a display directly readable by humans includes a credit or identification card containing: a timing device; an encryption code which is unique for each card; a method for displaying an encrypted code which is derived from the time at which the card is used; a display on the card which is readable by humans and current bar code hardware, said display can display the card's time, card number, and encrypted code number.

In another aspect of the present invention, a serial code, showing the number of uses of the card can be substituted for the timing device.

In another aspect of the present invention, the device can also have a control mechanism for turning on the card or the card's display which enhances the card's security using methods such as using a PIN number or a fingerprint.

In another aspect of the present invention, a portable electronic device with a display can be substituted for the credit card or identification card.

DESCRIPTION OF THE DRAWINGS

Other objects, features and advantages of the invention will become readily apparent upon reference to the following detailed description when considered in conjunction with the accompanying drawings, in which like reference numerals designate like parts throughout the figures thereof, and wherein:

FIG. 1 is a high level functional flowchart of an exemplary preferred embodiment of the present invention.

FIG. 2 is a functional flowchart illustrating steps of an exemplary preferred method for usage of a credit card, debit card, or ATM card.

FIG. 3 is a functional flowchart illustrating steps of providing card or account information for different methods of making financial transactions using a credit card, debit card, or ATM card.

FIG. 4 is a chart showing methods of inputting information from the card for various purchase methods and types of cards.

FIG. 5 is a detailed drawing of an exemplary credit card, debit card, ATM card or identification card which uses a PIN number to access the card.

FIG. 6 is a functional flowchart showing usage of an identification card.

FIG. 7 displays a method of generating secure information for internet logins or transactions.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

An exemplary preferred embodiment of the present invention is adapted to provide a method for creating and using credit cards, debit cards and ATM cards which have improved resistance to fraud and theft using encryption and time codes within the cards themselves. A second embodiment is included for similar cards which are designed to provide identification or security access. A third embodiment is included for using similar procedures to enhance security for internet or local area network password access.

Major Inputs and Outputs

Referring to FIG. 1, an exemplary preferred system 100 according to the present invention includes a digital computing device 101, for example, a smart card with and LCD display, a Palm Pilot, or a personal computer. The digital computing device 101 has a bar code display 103, a keypad or user identification detector 105, and is programmed with an encryption algorhythm 107. The keypad or user identification detector 105, can take many forms, such as a keypad which accepts a password or a pin number, a fingerprint reader, or a retinal scanner. The bar code display 103 is optional and is used only for certain applications.

A unique encryption key 109 is used for each installation, account, or digital computing device. The digital computing device 101, uses several inputs. Access information 111, such as a pin number or fingerprint, is used to obtain access to the digital computing device 101. One or more card numbers or account numbers 113 are stored on the digital computing device 101. The current time at each use 115 is obtained from an internal clock.

For many applications, a readout on a bar code display 103, is scanned by a bar code scanner 117 and the information is transmitted to a seller or security system 119. In other applications, information is sent directly from the digital computing device 101 to the seller or security system 119. The seller or security system 119 also uses seller or security information 121. Such information might include a store name, a merchant number, or a security access number. Information regarding items to be purchased or access being requested is also input 123.

Information from the seller or security system 119, is sent as an authorization request 125 to a transaction authorization center 127. Such authorization center might be a credit card authorization center, a center for security clearance, or a bank. The transaction authorization center 127 also uses data regarding account numbers or card numbers 129, encryption keys 131, authorization levels 133, transaction records 135, identification information 137 and one or more encryption algorhythms 139. The transaction information center generates authorization approvals or denials 141. After a transaction is completed, transaction records 135 are updated, and any appropriate changes are made in authorization levels 133.

Financial Transactions in Person

FIG. 2 illustrates steps of an exemplary preferred method 200 for usage of a credit card, debit card, or ATM card. In order to access the card and attempt a transaction, card access information 203 is provided by the user and compared with access information on the card itself to determine if both sets of information match 201. Card access information can come in many forms. For example, access information might involve a PIN number, a password, a fingerprint, voice activation, a retinal image, or an old-

fashioned metal key. For high-security applications, multiple types of access info might be required on the same card, such as both voice activation and a PIN number.

For some applications, cost effectiveness might dictate making a card with no access control mechanism. Such a card would have access similar to a current plastic credit card, which is always "on"; a current plastic card's information is always available, regardless of who has possession of the card. On current credit cards, the card's information is available even when lost, stolen, or "borrowed" by friends or family members. Once a card has a display which is capable of changing, nothing prevents use of the same card for multiple accounts. Different accounts might be accessed from the same card with different PIN numbers, for example.

If the access information does not match at 201, a "no" advances to 207 where a decision is made regarding retrying providing access information for the card. If the user would like to retry accessing the card, a "yes" advances to 209 and allows the user to retry providing card access information 201. If there is concern about whether an improper person is attempting to access the card, concern about whether the card is valid, or concerns about whether the card may be an attempted copy or counterfeit, a "no" advances to 211, where a security or valid card check is performed.

If card access information 201 does match, the card itself provides information 205 which may include: card number, account number, cardholder name(s), expiration date, usage restriction information, date according to the card's clock, time according to the card's clock, number of times the card has been used, and an encrypted code related to such information.

For technical reasons, it is likely that the encrypted code will be related to number of card uses, time or time and date information. The card information and an encrypted code related to that information will be used to confirm that the card is an original and in the physical possession of the cardholder at the time a transaction is attempted. The encrypted information should vary from one attempted transaction to the next in a way which the transaction center will be able to confirm, but forgers and thieves cannot usefully guess, intercept or copy.

For example, the encrypted code might be based on year, month, day, hour, minute, and second at which the card is accessed. In this case, even the fastest users would access the card a few seconds later for the next attempted transaction. The card's time would change, as would the encrypted code based on the time. This encrypted code would change in a way which is not predictable to anyone who does not have the encryption key for that particular card. Most likely, the encryption key is only stored in two places: on the user's card, in a manner which is very difficult or impossible to get to without possessing and mutilating the card; and on the information system of the transaction center.

It is this additional bit of changing encrypted data which cannot be easily guessed that will reduce or eliminate certain types of credit card fraud. Credit card slips from prior charges are useless for attempting new charges, since they do not provide the new encrypted data required for a subsequent transaction. Similarly, account statements, receipts, photocopies of a card, intercepted internet orders, and card numbers overheard during a phone order are rendered useless to potential thieves.

The card itself can provide information 205 in a variety of ways. Several different methods are shown in FIG. 3. The "card" can even be a program on a handheld computing device or a computer. One preferential embodiment is a card of similar size to a current credit card where information is displayed on a liquid crystal display (LCD), a detail drawing of which is shown in FIG 5. This LCD can display data in a form directly readable by humans and by bar code scanners. Thus, the card can be used in person, for phone orders, and for internet orders with similarly high levels of security.

The merchant will input additional information regarding purchases 215 and the merchant 217. This merchant information is bundled along with information provided by the card 213 and transmitted to the authorization center 219. The data transmitted to the authorization center can be similar to data transmitted using current methods, except that encrypted data which changes with each use of the card is included.

The transaction center will use information on current valid account numbers or card numbers, encryption keys, and any identification information which might also be transmitted 223 to determine whether the requested transaction involves a current and

valid card 221. If the card is not current or valid, a "no" results in the card being declined 225.

If the card is current and valid, a "yes" causes the transaction center to determine if the charge is allowable 227. Determining if a charge is allowable can be done using current means which compare the requested transaction with information such as available balances and authorization levels 229. If the charge is not allowable, the transaction is declined 231. If the charge is allowable, the transaction center accepts the transaction 233 and makes any necessary updates in records and authorization levels 235.

Note that this method of using encrypted data based authorization is also backward compatible. It is possible for a transaction authorization center to authorize current plastic cards and encryption based cards concurrently. Encryption based cards would have a much better level of security, but the same system could be used for traditional plastic cards. For plastic cards, the steps for input and matching of encrypted data are simply ignored, or the system effectively treats all plastic cards as if they had an encryption code which always matches.

Methods of Providing Card or Account Information

FIG. 3 illustrates steps of providing card or account information for different methods of making financial transactions using a credit card, debit card, or ATM card. As mentioned above, the "card" can also be a program on a handheld computing device or a computer.

The method of providing information depends on the method by which merchandise or services are being purchased, for example: in person, via phone, or via the internet 301. If the method of purchase is in person, the method of providing data depends on whether the merchant uses a bar code scanner 305. If "yes" the merchant will scan the bar code display on the card 307, which includes encrypted data as described in FIG. 2. Since a handheld computing device or a computer can display bar codes, these can also be used in place of the card. If the merchant does not use a bar code scanner, the card information can be read and input by a cashier, waiter, salesperson, clerk, etc. 309. Inputting card information by hand also works as a fallback or transitional method for a

merchant whose bar code system is not yet programmed for reading credit cards, or whose system is temporarily down.

For internet orders, the user will have different card or account information input procedures depending on whether the user has a virtual card program on his or her computer 311. Similar methods to those used to create a encryption-based card with a display can be used to create a program on a computer which functions in a like manner.

Any computer connected to the internet, a local area network, or similar communications system will require safeguards to prevent unauthorized copying of such a program. There are an assortment of such unauthorized copying safeguards which are familiar to computer programmers and computer manufacturers. Certain synergies become possible if the card is replaced by a program on the user's computer. One such synergy is the ability to integrate the card-emulation program with accounting or tax software. This integration would be popular with businesses whose employees make large numbers of expense account purchases and individuals who wish to simplify bookkeeping.

If a card-emulation program runs on the user's computer, a "yes" advances to 313, where card or account information for a purchase is made directly from the user's computer. If the user is not running a card-emulation program, the user keys in card or account information by hand 315. Regardless of which method is used for inputting purchase information via the internet, enhanced information security will result. If a credit card transaction is intercepted, or information from a website is accessed by unauthorized persons, information from prior transactions is useless in attempts at later fraudulent transactions.

For phone transactions, the method of inputting data is different depending on whether data is taken by a live human representative 317. If information is being taken by a live representative, the representative keys in said information 319. If the information is not taken by a live representative, a "no" at 317 advances to another decision regarding whether the information is entered by the user on the user's phone keypad or is spoken by the user and analyzed by voice recognition software 321. If the method is "keypad", the user keys in card or account information on their phone's keypad

323. For "voice", the user says the necessary information and voice recognition 325 translates the necessary data.

Methods of Inputting Card Information

FIG. 4 is a chart showing methods of inputting information from the card for various purchase methods and types of cards. Such information might include: card number, account number, cardholder name(s), expiration date, usage restriction information, date according to the card's clock, time according to the card's clock, number of times the card has been used, and an encrypted code related to such information.

As can be seen from FIG. 4, the "card" may be embodied on: a card with a display, such as an LCD; a handheld computing device, such as a Palm Pilot; a laptop, notebook, or other personal computer; or a home or office computer.

It is to be understood that the "cashier" listed in FIG. 4 can also be a clerk, waiter, salesperson, or anyone else capable of accepting an in person transactions, and that the "rep" can also be a telemarketer, salesperson, or anyone else capable of accepting a phone transaction.

Drawing of Exemplary Card

FIG. 5 is a detailed drawing at 2X scale of an exemplary credit card, debit card, ATM card or identification card which uses a PIN number to access the card. The keypad at the top of the card is used for inputting the PIN number and can be replaced with a voice recognition unit, a fingerprint sensor, a retinal scanner, or any other method of confirming the identity of the user.

The first 16 digits of the first row of bar codes contains the card number and the last four contain the expiration date. The second row of bar codes contains the date and time, in this case 06/08/2003 at 09:43:02 a.m., and an encrypted code which changes with each use. At the bottom of the card is the cardholder name and issuer name.

It is not necessary to display any information permanently on the card. However, since many individuals may carry more than one card and different individuals will have

similar cards, displaying some information permanently on the card is usually desirable. Of course, cards can be printed with various colors, patterns, or designs which do not directly convey specific information but allow a user to easily find the card in their purse or wallet.

As mentioned above regarding step 201, it is also possible to create cards with no access control mechanism. In that case, control of access to the card is similar to current plastic credit cards. Many variations can be implemented for size, placement of elements of the card, the method of displaying a changeable bar code, and the method of accessing the card.

Second Embodiment for Identification Cards and Security Access

FIG. 6 is a functional flowchart showing usage of an identification card. In order to access the card and attempt a transaction, card access information 603 is provided by the user and compared with access information on the card itself to determine if both sets of information match 601. Card access information can come in many forms. For example, access information might involve a PIN number, a password, a fingerprint, voice activation, a retinal image, or an old-fashioned metal key. For high-security applications, multiple types of access info might be required on the same card, such as both voice activation and a PIN number.

If the access information does not match at 601, a "no" advances to 607 where a decision is made regarding retrying providing access information for the card. If the user would like to retry accessing the card, a "yes" advances to 609 and allows the user to retry providing card access information 601. If there is concern about whether an improper person is attempting to access the card, concern about whether the card is valid, or concerns about whether the card may be an attempted copy or counterfeit, a "no" advances to 611, where a security or valid card check is performed.

If card access information 601 does match, the card itself provides information 605 which may include: card number, access level, access time restrictions, account number, cardholder name(s), expiration date, usage restriction information, date

according to the card's clock, time according to the card's clock, number of times the card has been used, and an encrypted code related to such information.

The card itself can provide information 605 in a variety of ways. Several different methods are shown in FIG. 3. The "card" can even be a program on a handheld computing device or a computer. One preferential embodiment is a card of similar size to a current credit card where information is displayed on a liquid crystal display (LCD), a detail drawing of which is shown in FIG 5. This LCD can display data in a form directly readable by humans and by bar code scanners.

The information on the card is input into a local verification system or transmitted to a remote verification system 613. An example of a local verification system would be the security desk for access to an office building. Examples of remote verification systems might be the Social Security Administration verifying that a Social Security Card is valid, a State verifying that a driver's license is valid, a university verifying student identification to access a computer center, and a gym verifying a membership card.

Information input into the verification system 613 is checked to see if the card is current and valid 615, using a database including information such as: current valid card numbers, encryption keys, or identification information. If the card is not valid, a "no" at 615 will cause the verification system to decline the identification 619.

If the card is current and valid, a "yes" causes the verification system to determine if the requested access is allowable 621. Such access might be restricted by time, facility, use, etc. If the access is not allowable, the access is declined 625. If the access is allowable, the verification system accepts the transaction 627 and makes any necessary updates in records 629.

Virtually any characteristic of a smart card used for security or access can be integrated into cards with encryption-based fraud protection.

Third Embodiment for Internet or Local Area Network Access

A similar mechanism to encryption-based fraud protection for credit cards can be used for security on internet logins or internet financial transactions. It works very well if

the user always works from the same computer or the same few computers. Such a login method will prevent the interception of passwords in transit. Passwords would have to be stolen by accessing the encryption program on the computer. The encryption program can also be external to the computer. It can be stored on a CD, DVD, floppy disk, USB device, or any other item which allows data to be read by the computer.

The advantage of using encryption-based fraud protection for internet logins or internet financial transactions is that critical access or authorization information cannot be intercepted in internet transmissions. For example, if a password allows access to an internet account with a pharmacy and the password and account information are intercepted, someone might be able to get a prescription for a controlled substance delivered to an addict's address instead of being delivered to the person for whom it is prescribed. Online banking, online brokerage, and online merchants will all derive benefits from additional security of logins and transaction authorization. If information sent to validate access is only useful one time, many forms of internet theft, fraud, invasion of privacy, and harassment disappear. Many forms of internet fraud involve breaking into databases of credit card information. If additional data beyond the credit card number is required for each new transaction, accessing large databases of credit card numbers is much less productive for thieves.

FIG. 7 is a functional flowchart showing usage of an internet access program located on a computer accessible to the user. The program functions in many ways like the encryption-based card described in FIG. 2.

In order to access the program and attempt a login or transaction, access information 603 is provided by the user's computer and compared with access information on a website or at an authorization center to determine if both sets of information match 701. Access information can come in many forms. For example, access information might involve a PIN number, a password, a fingerprint, voice activation, a retinal image, or an old-fashioned metal key. For high-security applications, multiple types of access info might be required on the same card, such as both voice activation and a PIN number.

If the access information does not match at 701, a "no" advances to 707 where a decision is made regarding retrying providing access information from the computer. If the user would like to retry access, a "yes" advances to 709 and allows the user to retry providing computer access information 701. If there is concern about whether an improper person is attempting to use the computer, concern about whether the card-emulation program is valid, or concerns about whether the program may be an attempted copy or counterfeit, a "no" advances to 711, where a security or valid program check is performed.

If card access information 701 does match, the computer program provides information 705 which may include: membership number, access level, access time restrictions, account number, cardholder name(s), expiration date, usage restriction information, date according to the card's clock, time according to the card's clock, number of times the card has been used, and an encrypted code related to such information.

The information provided by the computer program is transmitted to the website 713. Information transmitted to the website 713 is checked to see if the card is program is current and valid 715, using a database including information such as: current valid membership numbers, encryption keys, or identification information. If the program is not current or valid, a "no" at 715 will cause the website to decline the identification 719.

If the program provides information which is current and valid, a "yes" causes the verification system to determine if the requested access is allowable 721. Such access might be restricted by time, website, authorization level, etc. If the access is not allowable, the access is declined 725. If the access is allowable, the website accepts the transaction 733.

I Claim:

1. A portable device suitable for use in financial transactions, with a self contained means for displaying information which may change from one use of the card to the next comprising:

A self-contained means for displaying information which is readable by both humans and electronic devices.

2. A portable device suitable for use in financial transactions, with a self contained means for providing a time code or serial number of transaction code comprising:

A self contained means for calculating said serial number of transactions or time code and an encrypted value calculated in consideration of said serial number of transactions or time code.

3. A portable device suitable for use in financial transactions, with a self contained means for displaying information regarding a time code or a serial number of transaction code comprising:

A self contained means for calculating and displaying said serial number of transactions or time code and an encrypted value calculated in consideration of said serial number of transactions or time code.

4. A portable device suitable for use in authorizing access, with a self contained means for providing a time code or serial number of transaction code comprising:

A self contained means for calculating said serial number or time code and an encrypted value calculated in consideration of said serial number or time code.

5. A portable device suitable for use in authorizing access, with a self contained means for displaying information which may change from one use to the next comprising:

A self-contained means for displaying information which is readable by both humans and electronic devices.

6. A program suitable for use on a computer or other device for accessing the internet wherein said program includes:

a method for accessing user or account information;

a method for accessing a time code;

a method for calculating an encrypted value in consideration of time codes; and,

a method for transmitting said user or account information, time codes, and an encrypted value calculated in consideration of time codes.

7. The program of claim 6 wherein the program further includes:
a method for controlling access to the program on a user's computer.

8. The program of claim 7 wherein:
the method for controlling access is a PIN number.

9. The program of claim 7 wherein:
the method for controlling access is a password.

10. The program of claim 7 wherein:
the method for controlling access is a physical key.

11. The program of claim 7 wherein:
the method for controlling access is one or more questions asked of the user.

12. The program of claim 7 wherein:
the method for controlling access is insertion of a disk with particular content.

13. The program of claim 7 wherein:
the method for controlling access allows access only at particular times.

14. The program of claim 7 wherein:
the method for controlling access allows access to only one website.

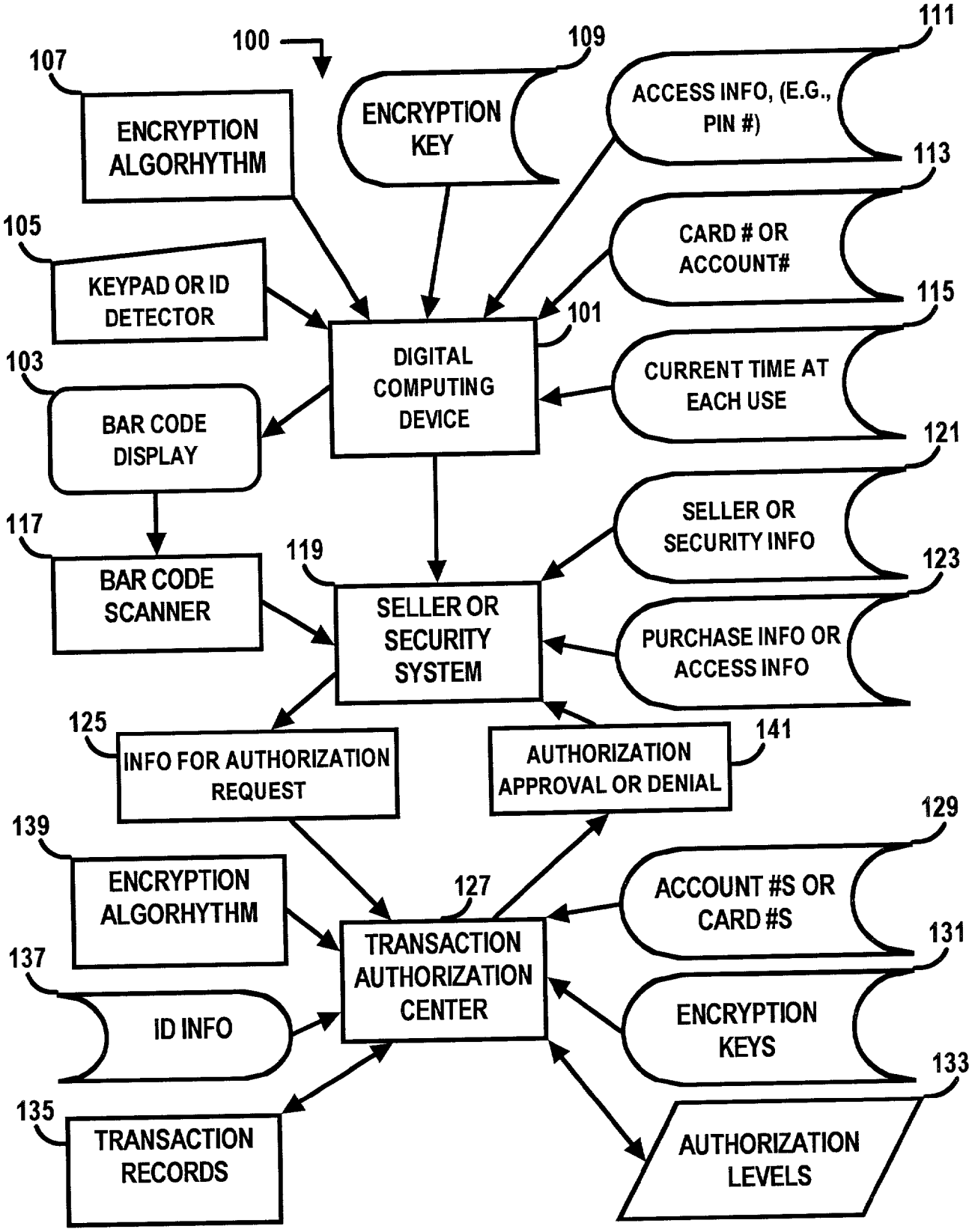
100
107
ENCRYPTION ALGORHYTHM
109
ENCRYPTION KEY
111
ACCESS INFO, (E.G., PIN #)
113
CARD # OR ACCOUNT#
115
CURRENT TIME AT EACH USE
105
KEYPAD OR ID DETECTOR
101
DIGITAL COMPUTING DEVICE
103
BAR CODE DISPLAY
121
SELLER OR SECURITY INFO
117
BAR CODE SCANNER
119
SELLER OR SECURITY SYSTEM
123
PURCHASE INFO OR ACCESS INFO
125
INFO FOR AUTHORIZATION REQUEST
141
AUTHORIZATION APPROVAL OR DENIAL
139
ENCRYPTION ALGORHYTHM
127
TRANSACTION AUTHORIZATION CENTER
129
ACCOUNT #S OR CARD #S
131
ENCRYPTION KEYS
137
ID INFO
133
AUTHORIZATION LEVELS
135
TRANSACTION RECORDS

FIG. 1

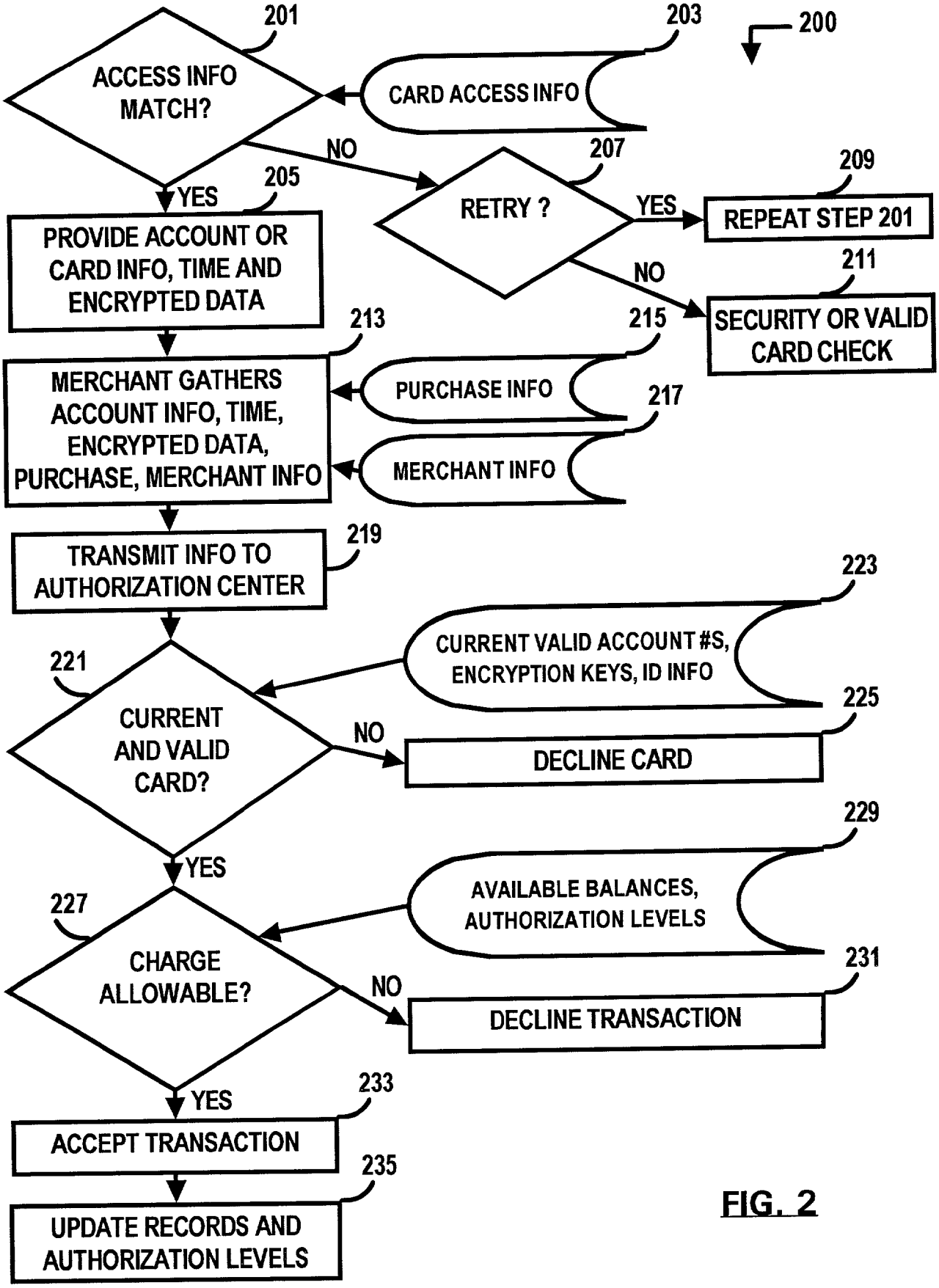
200
201
ACCESS INFO MATCH?
203
CARD ACCESS INFO
NO
207
RETRY ?
YES
209
REPEAT STEP 201
NO
211
SECURITY OR VALID CARD CHECK
YES
205
PROVIDE ACCOUNT OR CARD INFO, TIME AND ENCRYPTED DATA
213
MERCHANT GATHERS ACCOUNT INFO, TIME, ENCRYPTED DATA, PURCHASE, MERCHANT INFO
215
PURCHASE INFO
217
MERCHANT INFO
219
TRANSMIT INFO TO AUTHORIZATION CENTER
223
CURRENT VALID ACCOUNT #S, ENCRYPTION KEYS, ID INFO
221
CURRENT AND VALID CARD?
NO
225
DECLINE CARD
YES
229
AVAILABLE BALANCES, AUTHORIZATION LEVELS
227
CHARGE ALLOWABLE?
NO
231
DECLINE TRANSACTION
YES
233
ACCEPT TRANSACTION
235
UPDATE RECORDS AND AUTHORIZATION LEVELS

FIG. 2

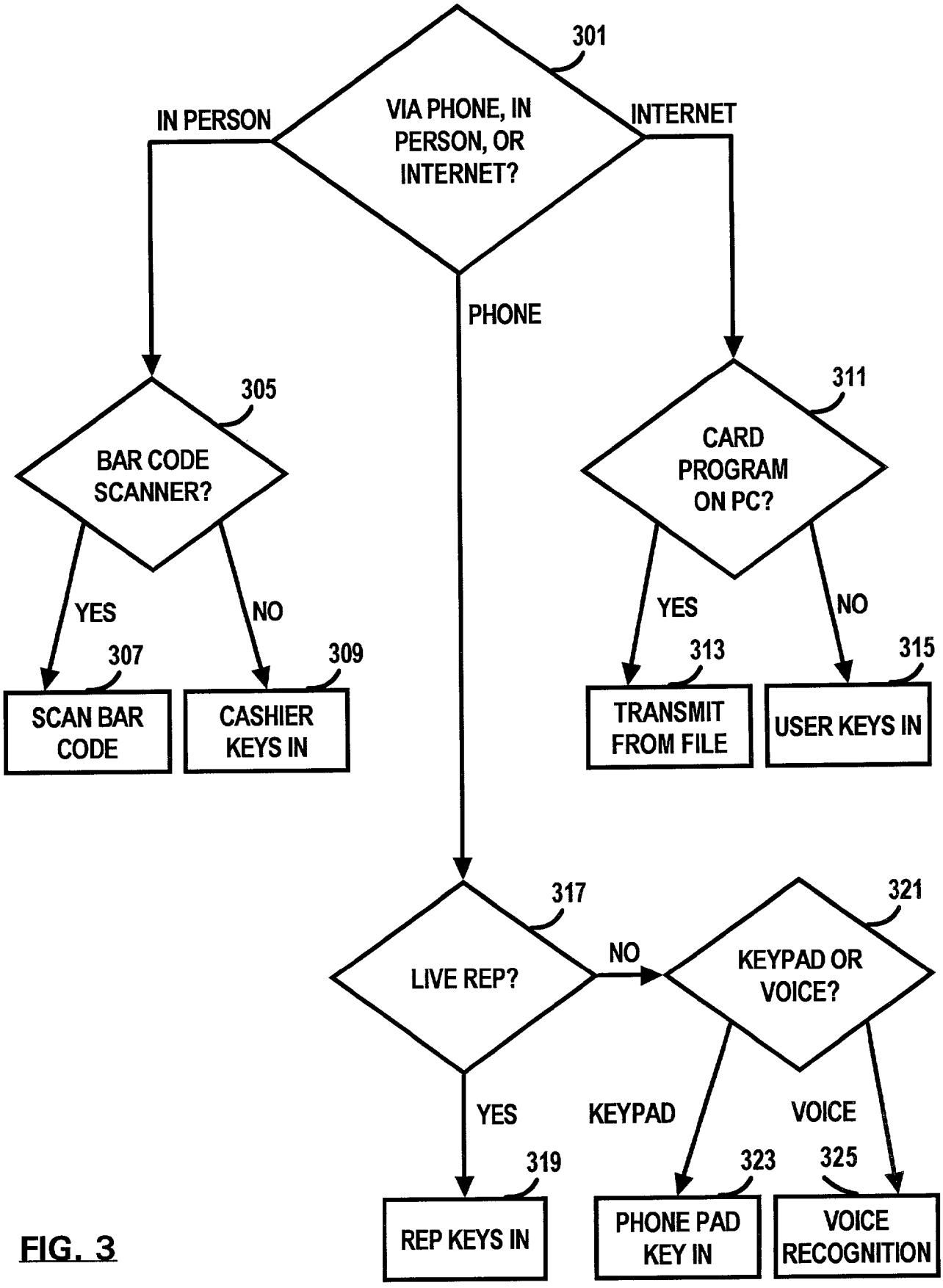
301
VIA PHONE, IN PERSON, OR INTERNET?
IN PERSON
INTERNET
PHONE
305
BAR CODE SCANNER?
YES
NO
307
SCAN BAR CODE
309
CASHIER KEYS IN
311
CARD PROGRAM ON PC?
YES
NO
313
TRANSMIT FROM FILE
315
USER KEYS IN
317
LIVE REP?
NO
321
KEYPAD OR VOICE?
YES
KEYPAD
VOICE
319
REP KEYS IN
323
PHONE PAD KEY IN
325
VOICE RECOGNITION

FIG. 3

FIG. 4

METHODS OF INPUTTING CARD INFORMATION

"CARD" EMBODIED ON	PURCHASE METHOD		
	IN PERSON	PHONE	INTERNET
CREDIT CARD WITH LCD DISPLAY	BAR CODE SCANNER KEYED IN BY CASHIER	CARDHOLDER TO REP. PHONE KEYPAD VOICE RECOGNITION	KEYED IN BY CARDHOLDER
HANDHELD COMPUTING DEVICE	BAR CODE SCANNER KEYED IN BY CASHIER	CARDHOLDER TO REP. PHONE KEYPAD VOICE RECOGNITION	KEYED IN BY CARDHOLDER DIRECT TRANSMISSION FROM FILE
LAPTOP, NOTEBOOK, PORTABLE COMPUTER	BAR CODE SCANNER KEYED IN BY CASHIER	CARDHOLDER TO REP. PHONE KEYPAD VOICE RECOGNITION	DIRECT TRANSMISSION FROM FILE KEYED IN BY CARDHOLDER
HOME OR OFFICE COMPUTER	NOT LIKELY	CARDHOLDER TO REP. PHONE KEYPAD VOICE RECOGNITION	DIRECT TRANSMISSION FROM FILE KEYED IN BY CARDHOLDER

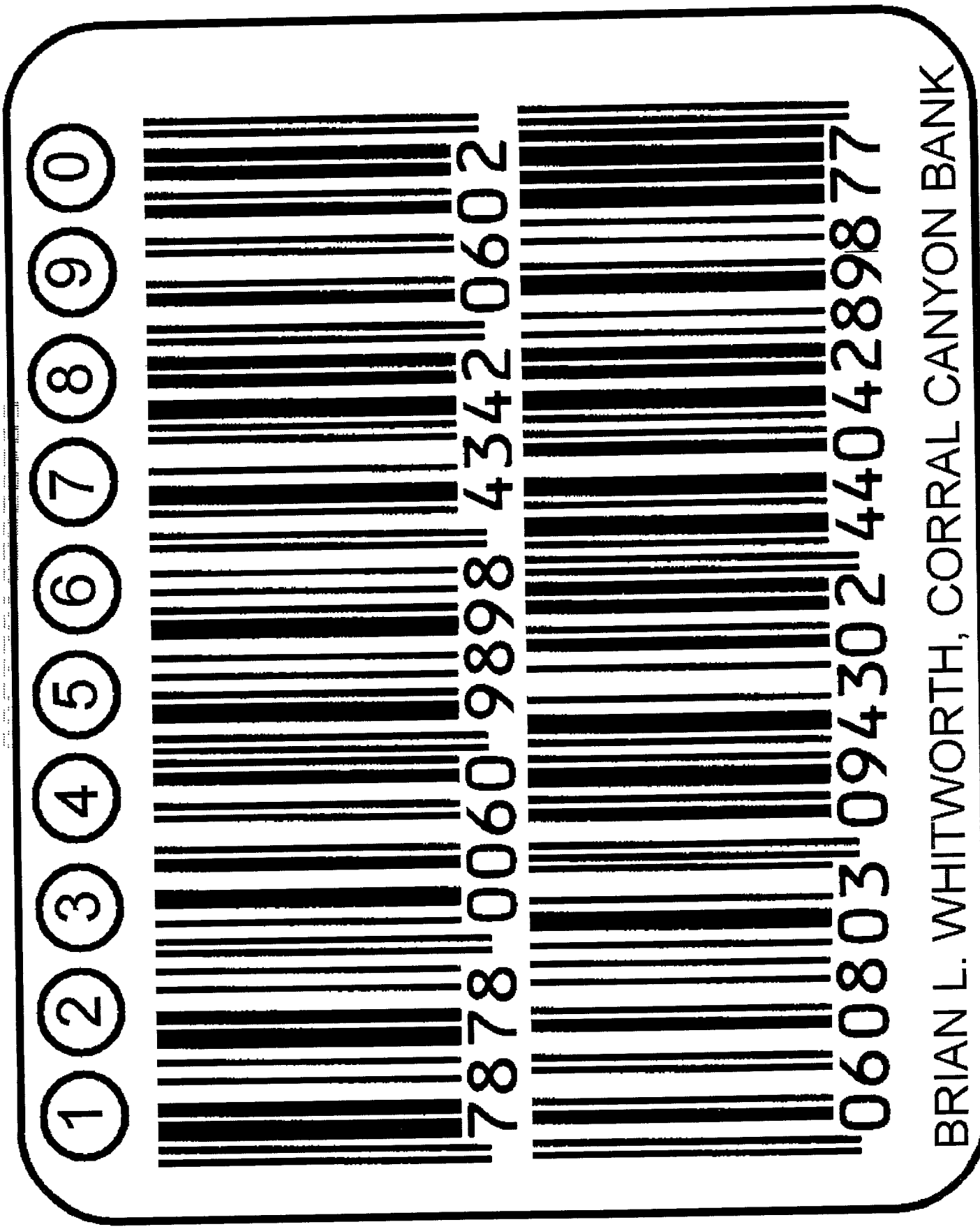
1 2 3 4 5 6 7 8 9 0
7878 0060 9898 4342 0602
0608 03 0943 0244 0428 9877
BRIAN L. WHITWORTH, CORRAL CANYON BANK

FIG. 5

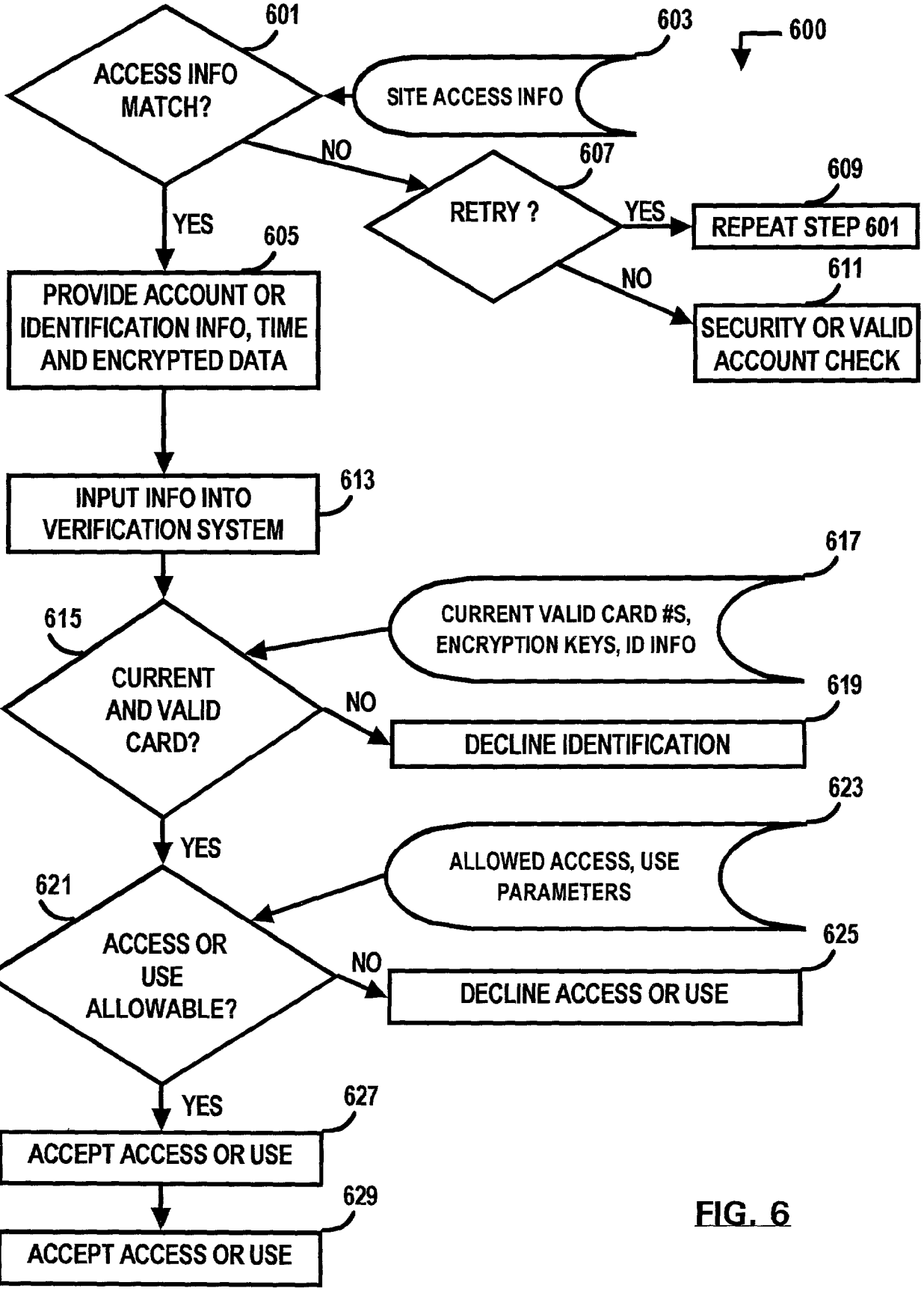
600
601
ACCESS INFO MATCH?
603
SITE ACCESS INFO
NO
607
RETRY ?
YES
609
REPEAT STEP 601
NO
611
SECURITY OR VALID ACCOUNT CHECK
YES
605
PROVIDE ACCOUNT OR IDENTIFICATION INFO, TIME AND ENCRYPTED DATA
613
INPUT INFO INTO VERIFICATION SYSTEM
617
CURRENT VALID CARD #S, ENCRYPTION KEYS, ID INFO
615
CURRENT AND VALID CARD?
NO
619
DECLINE IDENTIFICATION
YES
623
ALLOWED ACCESS, USE PARAMETERS
621
ACCESS OR USE ALLOWABLE?
NO
625
DECLINE ACCESS OR USE
YES
627
ACCEPT ACCESS OR USE
629
ACCEPT ACCESS OR USE

FIG. 6

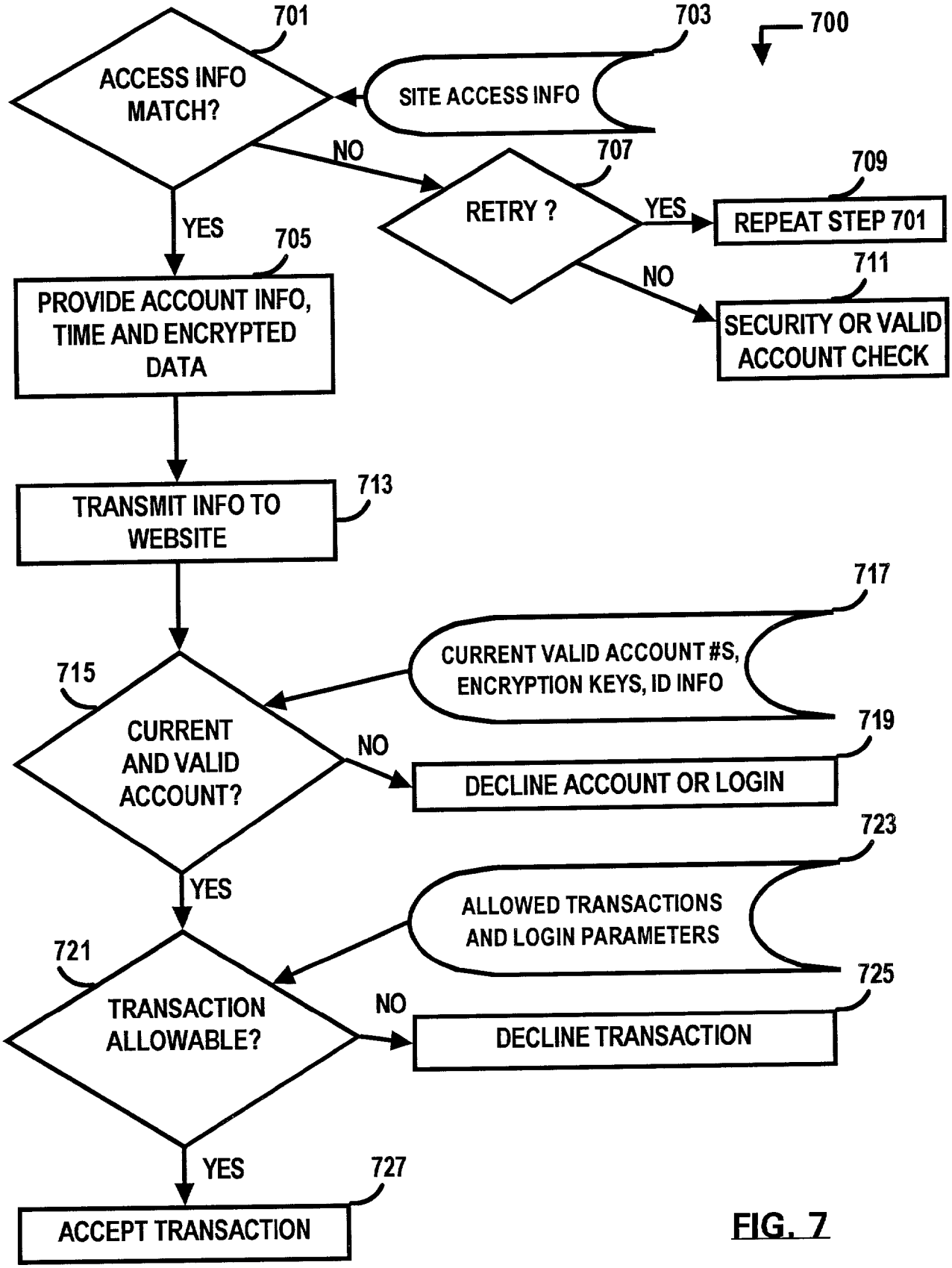
700
701
ACCESS INFO MATCH?
703
SITE ACCESS INFO
NO
YES
707
RETRY ?
YES
709
REPEAT STEP 701
NO
711
SECURITY OR VALID ACCOUNT CHECK
705
PROVIDE ACCOUNT INFO, TIME AND ENCRYPTED DATA
713
TRANSMIT INFO TO WEBSITE
717
CURRENT VALID ACCOUNT #S, ENCRYPTION KEYS, ID INFO
715
CURRENT AND VALID ACCOUNT?
NO
719
DECLINE ACCOUNT OR LOGIN
YES
723
ALLOWED TRANSACTIONS AND LOGIN PARAMETERS
721
TRANSACTION ALLOWABLE?
NO
725
DECLINE TRANSACTION
YES
727
ACCEPT TRANSACTION

FIG. 7